UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,955	12/08/2006	Taizo Shirai	288677US8PCT	3692

22850 7590 05/13/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
05/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/577,955	**Applicant(s)** SHIRAI ET AL.	
	Examiner KAVEH ABRISHAMKAR	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *5/2/06, 1/24/08, 10/15/08, 3/2/09*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on May 2, 2006. Claims 1-13 were originally received for consideration. No preliminary amendments for the claims were received.

2. Claims 1-13 are currently pending consideration.

Information Disclosure Statement

3. Initialed and dated copies of Applicant's IDS (form 1449), received on 5/2/06, 1/24/08, and 3/2/09, are attached to this Office Action.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-6 are deemed non-statutory because the claims are interpreted as being purely software per se. Data structures or computer programs not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33

F.3d at 1361,31 USPQ2d at 1760. Both claims just provide for computer programs which are loaded into a device, and such claimed computer programs do not define any structural and functional interrelationship between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions (see Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility: Annex IV).

5. Claims 7-12 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

6. Claim 13 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The aforementioned claim discloses a "computer program" which is interpreted as being software per se. The functionality of functional descriptive material is realized only when the functional descriptive material is claimed as being embodied on ***a computer readable medium*** and is claimed as executed by a computer component. The cited claim provides no tangible computer components that work in conjunction with the functional descriptive material to impart functionality and as a result the claims are not statutory because they fail the practical application requirement of § 101 by failing to provide a useful, concrete, and tangible result (see MPEP 2106).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4-8, 10-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Muratani et al. U.S. Patent 7,194,090)>

Regarding claim 1, Muratani discloses:

An cryptographic processing apparatus for performing Feistel-type common-key-block cryptographic processing, having

a structure that repeatedly executes an SPN-type F-function having a nonlinear conversion section and a linear conversion section over a plurality of rounds, wherein (Figure 20; column 17: lines 36-46, column 18, lines 6-13);

each of the linear conversion section of an F-function corresponding to each of the plurality of rounds is configured to perform linear conversion processing of an input of n bit outputted from each of the m nonlinear conversion sections, totally mn bit, as linear conversion processing that applies a square MDS (Maximum Distance Separable) matrix, at least in the consecutive odd-numbered rounds and in the consecutive even-numbered rounds, different square MDS matrices L.sub.a, L.sub.b are applied (Figure 22; column 10, lines 60-67, column 17, lines 56-61); and a matrix composed of m column vectors selected arbitrarily from column vectors constituting inverse matrices L.sub.a.sup.-1, L.sub.b.sup.-1 of the square MDS matrices is linearly independent (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Muratani discloses:

The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L.sub.a.sup.-1, L.sub.b.sup.-1 is a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Muratani discloses:

The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix that is composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices and is linearly independent (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Muratani discloses:

The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein
each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices is also a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Muratani discloses:

The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein
each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function (Figure 20; column 17: lines 36-46, column 18, lines 6-13);

is made up of a matrix composed of row vectors extracted from a matrix M' that is composed of row vectors selected from a square MDS matrix M including all elements constituting the plurality of square MDS matrices (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Regarding claim 7, Muratani discloses:

An cryptographic processing method for performing Feistel-type common-key-block cryptographic processing, comprising the steps of:

executing an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing repeatedly over a plurality of rounds (Figure 20; column 17: lines 36-46, column 18, lines 6-13); and

in the conversion processing of an F-function corresponding to each of the plurality of rounds, performing linear conversion for n bit outputted from the m nonlinear conversion sections, totally mn bit, as linear conversion processing applying square MDS (Maximum Distance Separable) matrices (Figure 22; column 10, lines 60-67, column 17, lines 56-61); wherein

linear conversion processing with square MDS matrices such that at least in the consecutive even-numbered rounds and in the consecutive odd-numbered rounds different square MDS matrices L.sub.a, L.sub.b are applied, and a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L.sub.a.sup.-1, L.sub.b.sup.-1 of the square MDS matrices is linearly independent and makes up a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Muratani discloses:

The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

linear conversion processing by square MDS matrices such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L.sub.a.sup.-1, L.sub.b.sup.-1 is a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 10 is rejected as applied above in rejecting claim 7. Furthermore, Muratani discloses:

The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to the linear conversion processing of the F-function is such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices is linearly dependent and makes up a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Muratani discloses:

The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein each of the plurality of different square MDS matrices to be applied to linear conversion processing of the F-function is a square MDS matrix such that a matrix composed of m column vectors selected arbitrarily from the column vectors constituting the plurality of square MDS matrices becomes a square MDS matrix (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Claim 12 is rejected as applied above in rejecting claim 7. Furthermore, Muratani discloses:

The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to the linear conversion processing of the F-function is made up of a matrix composed of column vectors extracted from a matrix M' composed of row vectors selected from a square MDS matrix M that includes all elements constituting the plurality of square MDS matrices (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Regarding claim 13, Muratani discloses:

A computer program of performing the Feistel-type common-key-block cryptographic processing according to claim 7, comprising the step of:

executing an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing over a plurality of rounds (Figure 20; column 17: lines 36-46, column 18, lines 6-13), wherein the linear conversion processing of the F-function corresponding to each of the plurality of rounds is a linear conversion step of performing linear conversion processing for n bit outputted from them nonlinear conversion sections, totally mn bit, as linear conversion processing applying a square MDS (Maximum Distance Separable) matrix (Figure 22; column 10, lines 60-67, column 17, lines 56-61), and

in the linear conversion step, linear conversion processing by square MDS matrices is executed in such a way that at least in the consecutive even-numbered rounds and in the consecutive odd-numbered rounds, different square MDS matrices are applied, and a matrix composed of m column vectors selected arbitrarily from column vectors constituting inverse matrices L.sub.a.sup.-1, L.sub.b.sup.-1 of the square MDS matrices is linearly independent (Figure 20; column 17: lines 36-46, column 18, lines 6-13).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
05/09/2009
Primary Examiner, Art Unit 2431